

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries

Montero, Etienne; Van Enis, Quentin

Published in:
Computer Law and Security Review

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

[Link to publication](#)

Citation for pulished version (HARVARD):
Montero, E & Van Enis, Q 2011, 'Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle ?', *Computer Law and Security Review*, vol. 27, no. 1, pp. 21-35.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

available at www.sciencedirect.comwww.compseconline.com/publications/prodclaw.htm
**Computer Law
&
Security Review**

Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle?

Etienne Montero, Quentin Van Enis

University of Namur, Namur, Belgium

ABSTRACT

Keywords:

Internet intermediaries
Filtering measures
Human Rights
Content regulation

This study considers the scope of the injunction a court may issue against an intermediary service provider with a view to preventing or terminating an infringement, particularly of an intellectual property right. The matter is studied in the light of the aim shared by the European Union and the Council of Europe to promote freedom of expression via communication networks. Despite technological progress and the emergence of software that are increasingly precise and ever better controlled in terms of their effects, implementation of a filtering measure appears difficult to reconcile with the right to freedom of expression. Consequently, the problematic comes down to this question: how do we do enough without doing too much?

© 2011 Etienne Montero and Quentin Van Enis. Published by Elsevier Ltd. All rights reserved.

1. Introduction

It is not always simple to identify the authors of illegal or harmful content in an open digital environment, global in scale, where it is easy to operate from abroad and/or anonymously. On the other hand, intermediary providers involved in transmitting or storing the disputed content are known and clearly identified, close to the victim and generally solvent. It is therefore understandable that they have naturally become the preferred target of liability actions.

Thus the question of the liability of technical intermediaries with regard to illegal content transmitted or hosted by them has rapidly become a major issue when drawing up a legal framework for the information society. It is clear that one of the main objectives of the Directive on electronic commerce¹ was precisely to establish a system of exemption from liability for some Internet intermediary services.² It was

a matter of establishing a 'balance between the different interests at stake' (recital 41). Like the Digital Millennium Copyright Act on which it draws,³ the system of liability prescribed in Section 4 achieves a compromise between the interests of providers of Internet intermediary services and those of the content industry (creators and holders of rights to software, music, video, film, etc.).

A dual statement lies at the heart of this compromise. On the one hand, intermediary providers - confined to a purely technical role - are not supposed to acquaint themselves with the content they store or transmit; on the other hand, it is quite obvious that they are ideally placed and best equipped to prevent or terminate illegal practices committed via their services.

Hence the subtle arrangements put in place. On the one hand, exemptions from liability, based on conditions, are introduced for certain intermediary activities: transmission of

¹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJEC, L 178 of 17 July 2000, p. 1.

² In this regard, M. Peguera Poch, 'La exención de responsabilidad civil por contenidos ajenos en Internet' 2001, p. 1 (www.uoc.edu/in3/dt/20080/index.html).

³ For a more refined comparison of the two systems, E. Montero and H. Jacquemin, 'La responsabilité civile des médias', *Responsabilités - Traité théorique et pratique* (edited by J.-L. Fagnart), Book 26b, vol. 3, Brussels, Kluwer, 2004, Issue 189 et seq., p. 18 et seq.; R. Julia-Barcelo, 'On-line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Framework', *EIPR*, 2000, pp. 106–119; V. Sedallian, 'La responsabilité des prestataires techniques sur Internet dans le Digital Millennium Copyright Act américain et le projet de directive européenne sur le commerce électronique', *Cahiers Lamy droit de l'informatique et des réseaux*, Issue 110, 1999, pp. 1–4.

0267-3649/\$ – see front matter © 2011 Etienne Montero and Quentin Van Enis. Published by Elsevier Ltd. All rights reserved.

doi:10.1016/j.clsr.2010.11.012

information via a communication network, provision of access to such a network, storage of data in the form of a temporary copy ('cache') and hosting⁴; in addition, no *general* obligation may be imposed on these intermediary providers to monitor and supervise the content they transmit or store, nor any obligation actively to seek facts or circumstances indicating illegal activity.⁵ On the other hand, they are required to work with the judicial and police authorities by keeping them informed of alleged illegal activities carried out by recipients of their services or communicating to them the data identifying these recipients⁶; a court may impose a *temporary* monitoring obligation on them in a particular instance⁷ and an injunction is always possible, ordering a provider to prevent or terminate an infringement⁸; lastly, if alerted, providers of hosting and cache-copy services are also required to act expeditiously to remove the illegal content or disable access to it.⁹

Thus by shielding the intermediary providers from liability actions and not requiring them to undertake supervision and to track infringements themselves, the European legislator intended not just to encourage the boom in information society services but also to promote freedom of expression. In fact, if they were more exposed, they would be less inclined to develop potentially risky services such as those designed to receive content of all kinds supplied by Internet users. Undoubtedly, fewer community and participation sites would have emerged and flourished, including social networks (such as Facebook), wikis (such as Wikipedia) and blogs, content-sharing sites (such as YouTube and Dailymotion) or electronic marketplaces (such as eBay). Moreover, intermediary providers are spared the heavy costs linked to supervision and filtering¹⁰ - technically difficult to implement, of dubious effectiveness and involving significant cost - and all forms of prior censorship are avoided.

At the same time, it has been said, the interests of users and third parties are also taken into account since they are, in particular, at liberty to ask a court to order an intermediary to prevent or terminate an infringement. This possibility,

provided for by Directive 2000/31, has been confirmed in subsequent directives.¹¹

Case-law of recent years has indicated two main difficulties in interpreting the measure:

- the first relates to the advent of Web 2.0 services and whether the provider of such services may enjoy the exemption from liability prescribed for hosting activity¹²;
- the second concerns the scope of the injunction a court may issue against an intermediary with a view to preventing or terminating an infringement, particularly of an intellectual property right.

Only the latter question will be considered within this study.

In order to correctly interpret the provisions relating to liability of intermediaries, it is worth looking at the bigger picture and locating them within the legal framework common to the European Union and the Council of Europe. In fact, a shared desire may be seen on the part of the European Community and the 'Europe of Human Rights' to promote, via development of information technologies and communication networks, the information society and, more broadly, freedom of expression (I).

This objective of promoting freedom of expression is key to interpretation when determining the scope of injunctions liable to be issued against Internet intermediary providers (II).

2. Information society intermediaries, a medium for freedom of expression in the European legal order

Internet intermediaries play a cardinal role in promoting freedom of expression via communication networks. In this regard, the degree of concern on the part of the Council of Europe and the European Union to protect technical providers (A) is worthy of note. A close reading of Strasbourg case-law and the work of the Council of Europe confirms that they are clearly among the beneficiaries of the freedom of expression enshrined in Article 10 of the European Convention on Human Rights (B).

2.1. Convergence of concerns within the two Europes

Since the end of the 1990s both European Union and Council of Europe bodies have promoted the information society. This convergence of concerns is an excellent illustration of the dialogue established, many years ago from now, between the European Community and the Europe of Human Rights.

The two Europes are known to respond to one another on many issues. This phenomenon should be reinforced by the

⁴ Articles 12 to 14 of the Directive on electronic commerce.

⁵ Article 15(1) of the Directive on electronic commerce.

⁶ Article 15(2) of the Directive on electronic commerce.

⁷ Recital 47 of the Directive on electronic commerce.

⁸ Cf. Articles 12(3), 13(2) and 14(3), as well as recital 45, of the Directive on electronic commerce.

⁹ Articles 13(1)(e) and 14(1)(b) of the Directive on electronic commerce.

¹⁰ Filtering devices are 'content-control software applications designed to automatically block the display or downloading of selected material on a web browser or other Internet application' (C. Angelopoulos, 'Filtering the Internet for Copyrighted Content in Europe', *Iris plus*, 2009-4, p. 2 and the reference to COUNCIL OF EUROPE 'Report by the Group of Specialists on Human Rights in the information society (MC-S-IS) on the use and impact of technical filtering measures for various types of content in the online environment' CM(2008)37, available at www.tinyurl.com/adyzoz).

¹¹ Cf. Article 8(3) and recital 59 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJEC, L 167 of 22 June 2001, p. 10, as well as Article 11 and recitals 22 and 23 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJEU, L 195 of 2 June 2004, p. 16.

¹² On this question, see E. Montero, 'Les responsabilités liées au Web 2.0', RDTI, Issue 32, 2008, pp. 361–386; A. Saint Martin, 'Proposition d'une "responsabilité raisonnable" pour le Web 2.0', RLDI, 2007/32, No 1070, pp. 32–39; G. Teissonniere, 'Quelle responsabilité appliquer aux plates-formes de commerce en ligne et autres intermédiaires de contenus?', RLDI, 2008/35, No 1165, pp. 21–25.

entry into force of the Treaty of Lisbon, which took place on 1 December 2009 and gives binding force to the Charter of Fundamental Rights of the European Union,¹³ and by the scheduled accession of the latter to the European Convention on Human Rights.¹⁴

The Court of Justice of the European Union, with a view to reassuring some national constitutional courts that had shown resistance to applying Community law, has long considered itself competent to ensure respect, under general principles of European Union law, for fundamental rights as these result from the constitutional traditions common to the Member States and as guaranteed by the international instruments to which the Member States are party, among which the European Convention on Human Rights receives particular attention.

On the other hand, the European Court of Human Rights, led to supervise conformity with the Convention of certain measures adopted by States when executing obligations imposed by European Union law, has considered that transfer of competences to an international organisation cannot release a State from its responsibilities with regard to the Convention.¹⁵ Questionably, the Court acknowledged that, when a State had no discretion in applying Community law, its supervision had to be exercised with a degree of reserve.¹⁶ In such circumstances the Court will presume a State's compliance with the obligations incumbent on it under the Convention if the protection of fundamental rights provided by the international organisation may be held to be 'equivalent' to that provided by the mechanism of the Convention, as seems to be the case in the context of the European Community.

Drafting of the Directive on electronic commerce perfectly reflected this trend towards mutual dialogue between the two Europes by making explicit reference, in its seventh recital, to

freedom of expression as enshrined in Article 10 of the European Convention on Human Rights.

2.2. Internet intermediaries and Article 10 of the European Convention on Human Rights

2.2.1. The role of intermediaries and freedom of expression

Under Article 10 of the European Convention on Human Rights, 'everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (...)'. The second paragraph of the same Article 10 adds that 'the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary'.

Applying the guarantees under Article 10 to the digital universe does not appear to raise any obstacle of principle.¹⁷

In this regard, a Declaration of the Committee of Ministers of the Council of Europe expressly states that: 'Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form'.¹⁸

Quite to the contrary, the Internet, more than any other communication medium, harbours the possibility of a genuine 'public discussion space', the importance of which to the democratic project is well-known.¹⁹

The Committee of Ministers expresses itself thus in a recommendation to Member States: 'The development of information and communication technologies and services should contribute to everyone's enjoyment of the rights guaranteed by Article 10 of the European Convention on Human Rights, for the benefit of each individual and the democratic culture of every society'.²⁰

It is unquestionable, in the dawn of the 21st Century, that the net appears an essential medium for freedom of expression.

¹³ Article 11 of the Charter protects freedom of expression and information in the following way: '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.' The wording used is more condensed than that of Article 10 of the European Convention on Human Rights. Article 52 of the Treaty of Lisbon states, however, that 'insofar as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.' For a commentary, see E. Bribosia and O. De Schutter, 'La Charte des droits fondamentaux de l'Union européenne', *JT*, 2001, pp. 281–293, specifically pp. 284–285.

¹⁴ See Article 6(2) of the Treaty of Lisbon, which states that 'The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms (...). See E. Bribosia and O. De Schutter, *op. cit.*, pp. 288–289.

¹⁵ See ECtHR judgment in *Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v Ireland* of 30 June 2005, paragraphs 155–157. See also ECtHR judgment in *Matthews v United Kingdom* of 18 February 1999, paragraph 34.

¹⁶ See S. Adam and F. Krenc, 'La responsabilité des Etats membres de l'Union européenne devant la Cour européenne des droits de l'homme', *JT*, 2006, p. 87, paragraph 3.2.

¹⁷ See, in particular, P.-F. Docquir, 'Contrôle des contenus sur Internet et liberté d'expression au sens de la Convention européenne des droits de l'homme', *CDPK*, 2002, p. 174, Issue 1.

¹⁸ Declaration on Human Rights and the rule of law in the Information Society adopted by the Committee of Ministers on 13 May 2005 at the 926th meeting of the Ministers' Deputies, available at [sitewww.coe.int](http://www.coe.int).

¹⁹ See, in particular, the thesis, not yet published, by P.-F. Docquir, *La liberté d'expression dans le réseau mondial de communication : propositions pour une théorie du droit d'accès à l'espace public privatisé*, 2009.

²⁰ Declaration on Human Rights and the rule of law in the Information Society adopted by the Committee of Ministers on 13 May 2005 at the 926th meeting of the Ministers' Deputies, available at [sitewww.coe.int](http://www.coe.int).

Incidentally, moved for the first time to rule on an alleged infringement of freedom of expression via the Internet, the Strasbourg Supreme Court did not elaborate at all - as if it were obvious - concerning applicability of the guarantees under Article 10 to the Internet.²¹

As is well-known, the activity of intermediaries is essential to enable all to express themselves on the Web.

A progressive reading of the judgments delivered by the European Court of Human Rights in the field of Article 10 of the Convention should logically lead to an acknowledgement of the importance of technical intermediaries for freedom of expression.

In fact, the Court has, on many occasions, emphasised, with regard to publishers that, in supplying authors with a medium, they participate fully in freedom of expression and thus enjoy the guarantees offered by Article 10 of the Convention.²²

What is more, in a case concerning measures adopted by the Swiss State obstructing parabolic antenna reception of televised broadcasts transmitted via a Russian satellite, the Court affirmed that Article 10 protects both the content of information and the means of transmitting and receiving it, 'since any restriction imposed on the means necessarily interferes with the right to receive and impart information'.²³

Currently, digital media play a leading role among the 'means of transmitting and receiving information' and use of network intermediaries is a necessity for all those wishing to express themselves on the Web. Protecting intermediaries is therefore, at the same time, protecting freedom of expression.

2.2.2. Content protected by freedom of expression

Since the arrangements for exempting intermediaries that were put in place by the Directive on electronic commerce are based on the dual objective of encouraging electronic commerce and promoting freedom of expression, it seems worth recalling that the European Court of Human Rights

has expressly acknowledged that commercial speech is indeed classed as content protected by freedom of expression.²⁴

The Strasbourg Court emphasised in this regard that Article 10 of the Convention guarantees freedom of expression to 'everyone', without making a distinction according to whether the type of aim pursued is profit-making or not.²⁵ Thus, not just online publicity but also, for example, sales advertisements displayed in electronic marketplaces unquestionably come under content covered by Article 10 of the Convention.

2.2.3. Supervision of permissible restrictions

Interference in the right to freedom of expression may be directly the act of the State but may also result from its inability to provide persons under its jurisdiction with effective use of this right. In other words, under their positive obligations, States must take all reasonably proper measures to prevent freedom of expression being infringed.

Recalling the crucial importance of freedom of expression for democracy, the Court has affirmed that 'genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals'.²⁶

Transposed to the digital universe, this message should compel States to adopt a genuinely reassuring framework for intermediaries in order to avoid the private censorship they are liable to effect through fear of liability action.

In order to be permissible in terms of the Convention, any interference in the right to freedom of expression must meet the three cumulative conditions under the second paragraph of Article 10.

The first condition, that of legality, means that the State should state, clearly and precisely, in a norm accessible to all, those situations in which a restriction might apply so that individuals are able to determine, with an adequate level of foreseeability, the potential consequences of behaving in a particular way.²⁷

In order to meet the second condition, that of legitimacy, the restriction must pursue one of the legitimate objectives set out, restrictively, in the second paragraph of Article 10.

In the context of this study the objective that consists in protecting the reputation or the rights of others is of very particular significance.

In fact, injunctions, the scope of which will be analysed in the second part of this study, seek both to protect the honour and the private life of persons on the Web and to banish certain illegal content from it, in particular to ensure respect for intellectual property rights to a work.

As is often the case, a balance should therefore be struck between the interests involved. In this regard, in order to meet

²¹ ECtHR judgment in *Times Newspapers Ltd (Nos 1 and 2) v United Kingdom* of 10 March 2009, RDTI, issue 37, 2009, p. 87 and commentary by Q. Van Enis ('Le temps ne fait rien à l'affaire... Les archives Internet du Times devant la Cour européenne des droits de l'homme').

²² The analogy with technical intermediaries stops there since, in the absence of editorial work to select content, there can be no question of making them share the 'duties and responsibilities' incumbent on authors.

²³ ECtHR judgment in *Autronic AG v Switzerland* of 22 May 1990, paragraph 47. In a recent case the Court recalled that Article 10 applies to judicial decisions preventing a person from receiving information by satellite, ECtHR judgment in *Khurshid Mustafa and Tarzibachi v Sweden* of 16 December 2008, paragraph 32.

²⁴ See, in particular, ECtHR judgment in *Barthold v Germany* of 25 March 1985, paragraph 42. (In this case the Court, unable to distinguish between what counted as information and what counted as advertising, concluded that Article 10 was applicable 'without needing to inquire in the present case whether or not advertising as such comes within the scope of the guarantee under this provision'); ECtHR judgment in *Markt Intern Verlag GmbH and Klaus Beermann v Germany* of 20 November 1989, paragraph 26 (information of a commercial nature 'cannot be excluded from the scope of Article 10 § 1 which does not apply solely to certain types of information or ideas or forms of expression').

²⁵ See ECtHR judgment in *Casado Coca v Spain* of 24 February 1994, paragraph 35.

²⁶ ECtHR judgment in *Özgür Gündem v Turkey* of 16 March 2000, paragraph 43. See also ECtHR judgment in *Appleby and others v United Kingdom* of 6 May 2003, paragraphs 39–40.

²⁷ See, in particular, ECtHR judgment in *Sunday Times v United Kingdom* of 26 April 1979, paragraph 49; ECtHR judgment in *Stefanec v The Czech Republic* of 18 July 2006, paragraph 41.

the third and last condition, that of proportionality, the restriction must respond to a ‘pressing social need’ and be justified by ‘relevant and sufficient reasons’.²⁸

It is interesting to note in this regard that the Strasbourg Supreme Court considers that intellectual property rights come within the scope of Article 1 of the First Additional Protocol to the Convention, which enshrines the right to property.²⁹

Indeed, according to the Court, when the ‘rights and freedoms of others’, protection of which is seen as a legitimate objective, ‘are themselves among those guaranteed by the Convention or its Protocols, it must be accepted that the need to protect them may lead States to restrict other rights or freedoms likewise set forth in the Convention. It is precisely this constant search for a balance between the fundamental rights of each individual which constitute the foundation of a “democratic society”. The balancing of individual interests that may well be contradictory is a difficult matter, and Contracting States must have a broad margin of appreciation in this respect, since the national authorities are in principle better placed than the European Court to assess whether or not there is a “pressing social need” capable of justifying interference with one of the rights guaranteed by the Convention’.³⁰

Such balancing of freedoms concurrently enshrined by the Convention or by its Protocols must also be effected between the right to freedom of expression and the right to protection of private life guaranteed by Article 8 of the Convention.³¹

2.2.4. *The work of the Council of Europe as an interpretative background to Article 10 of the European Convention of Human Rights*

It is worth giving particular attention to the various texts, declarations and recommendations that have been adopted within the framework of the Council of Europe and greatly advance the objective of promoting freedom of expression in establishing a genuine information society.

²⁸ The case-law of the Court is settled in this regard. See, in particular, ECtHR judgment in *Sunday Times v United Kingdom*, cited above, paragraph 50. It seems worth recalling that according to the European Court of Human Rights, while prior restraints on publication are not, as such, prohibited by article 10 of the Convention, they call for the most careful scrutiny on the part of the Court. See, amongst others, ECtHR judgment in *Observer and v United Kingdom* of 26 November 1991, paragraph 60; ECtHR judgment in *Sunday Times v United Kingdom (n°2)* of 26 November 1991, paragraph 51; and, even more recently, ECtHR judgement in *Ürper and others v Turkey* of 20 October 2009, paragraph 39.

²⁹ See ECtHR (GC) judgment in *Anheuser-Busch Inc. v Portugal* of 11 January 2007, paragraphs 66 to 72, and, even more recently, ECtHR judgment in *Balan v Moldova* of 29 January 2008, paragraph 34.

³⁰ ECtHR judgment in *Chassagnou v France* of 29 April 1999, paragraph 113.

³¹ See ECtHR judgment in *Von Hannover v Germany* of 24 June 2004, paragraph 58.

³² Recommendation Rec(2001)8 of the Committee of Ministers to Member States on self-regulation concerning cyber content (cited above), for example, expressly states that ‘any Recommendation of the Committee of Ministers is an instrument of political commitment, and not a legally enforceable instrument. Through its adoption by the Committee of Ministers, it binds all Member States and does not require an individual adhesion by Member States’.

While this clearly concerns soft law, known *a priori* not to have any binding force,³² the importance of these texts should still not be underestimated.

In fact, the European Court of Human Rights, when needing to interpret the Convention, no longer has any hesitation in drawing on them, which gives them genuine indirect binding force.³³

According to the Court itself, it is its duty, when defining the meaning of terms and notions in the text of the Convention, to ‘take into account elements of international law other than the Convention, the interpretation of such elements by competent organs, and the practice of European States reflecting their common values. The consensus emerging from specialized international instruments and from the practice of Contracting States may constitute a relevant consideration for the Court when it interprets the provisions of the Convention in specific cases. In this context, it is not necessary for the respondent State to have ratified the entire collection of instruments that are applicable in respect of the precise subject matter of the case concerned. It will be sufficient for the Court that the relevant international instruments denote a continuous evolution in the norms and principles applied in international law or in the domestic law of the majority of Member States of the Council of Europe and show, in a precise area, that there is common ground in modern societies’.³⁴

This consideration should be kept in mind in order to properly appreciate the various texts referred to.

As early as 1999, the Committee of Ministers of the Council of Europe, in its Declaration on a European Policy for New Information Technologies,³⁵ called on the Member States to ‘encourage the free flow of information, opinions and ideas through the use of the new information technologies’ and to ‘ensure respect for Human Rights and human dignity, notably freedom of expression (...)’.

Two years later, the same Committee of Ministers adopted a Recommendation to Member States on self-regulation concerning cyber content.³⁶

The objective pursued by this text is evident from its recitals: it concerns protecting the freedom of expression of

³³ See, in particular, ECtHR (GC) judgment in *Demir and Baykara v Turkey* of 12 November 2008, paragraph 74. For a critical analysis see, in particular, F. Tulkens and S. Van drooghenbroeck, ‘Le soft law des droits de l’Homme est-il vraiment si soft? Les développements de la pratique interprétative récente de la Cour européenne des droits de l’Homme’ in *Liber amicorum Michel Mahieu*, Brussels, Larcier, 2008, pp. 505–526.

³⁴ ECtHR (GC) judgment in *Demir and Baykara v Turkey*, cited above, paragraphs 85–86.

³⁵ Declaration of the Committee of Ministers of the Council of Europe on a European Policy for New Information Technologies, adopted on 7 May 1999 at its 104th meeting, available at site www.coe.int.

³⁶ Recommendation Rec(2001)8 of the Committee of Ministers to Member States on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), adopted on 5 September 2001 at the 762nd meeting of the Ministers’ Deputies, available at site www.coe.int.

users when putting in place filtering measures against illegal or harmful content on the Internet.³⁷

In order for freedom of expression to be respected fully, filtering systems should therefore give users the opportunity 'to make qualified choices about the type of lawful content they wish to access, as for example parents or other persons or institutions having responsibility over children as to what content should be accessible to these children'.

Three years after adoption of the Directive on electronic commerce within the European Community, the Committee of Ministers of the Council of Europe adopted the Declaration on freedom of communication on the Internet.³⁸

In an interplay of cross-referencing, the Declaration recalls both the commitment of Member States of the Council of Europe in relation to the fundamental right to freedom of expression and information, as guaranteed by Article 10 of the European Convention on Human Rights, and the adoption of the Community Directive of 8 June 2000 by some of these States.

The Declaration includes a sixth principle, which enshrines the limited liability of service providers for Internet content.

In general terms, this principle stipulates that 'Member States should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity'.

With regard to host providers, this principle is formulated in the following way: 'In cases where (...) service providers (...) store content emanating from other parties, Member States may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information. When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information'.

In the Explanatory Note to the Declaration, it is further specified that: 'in the case of hosting content emanating from third

parties, intermediaries should in general not be held liable'. The text expressly refers to Article 14 of Directive 2000/31.

It is then specified that 'this does not apply (...) when the third party is acting under the control of the intermediary, for example when a newspaper company has its own server to host content produced by its journalists. However, if the host becomes aware of the illegal nature of the content on its servers or, in the event of a claim for damages, of facts revealing an illegal activity, it may reasonably be held liable. The precise conditions should be laid down in national law (...). It is to be expected that Member States will define in more detail what level of knowledge is required of service providers before they become liable. In this respect, so-called "notice and take down" procedures are very important. Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability'.

In 2005, by means of the Declaration on Human Rights and the rule of law in the Information Society,³⁹ the Member States of the Council of Europe undertook 'to adopt policies for the further development of the Information Society which are compliant with the ECHR and the case-law of the European Court of Human Rights, and which aim to preserve, and whenever possible enhance, democracy, to protect Human Rights, in particular freedom of expression and information, and to promote respect for the rule of law'.

In the Recommendation on promoting freedom of expression and information in the new information and communications environment,⁴⁰ adopted on 26 September 2007, the Committee of Ministers 'recommends that the governments of Member States take all necessary measures to promote the full exercise and enjoyment of Human Rights and fundamental freedoms in the new information and communications environment, in particular the right to freedom of expression and information pursuant to Article 10 of the ECHR and the relevant case-law of the European Court of Human Rights (...)'.
Lastly, in the Recommendation to Member States on measures to promote the respect for freedom of expression and information with regard to Internet filters,⁴¹ the Committee of Ministers, 'aware that any intervention by Member States that

³⁷ 'Recalling the commitment of the Member States to the fundamental right to freedom of expression and information as guaranteed by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and to entrusting the supervision of its application to the European Court of Human Rights; Reaffirming that freedom of expression and information is necessary for the social, economic, cultural and political development of every human being, and constitutes a condition for the harmonious progress of social and cultural groups, nations and the international community, as expressed in its Declaration on the Freedom of Expression and Information of 1982; Stressing that the continued development of new communications and information services should serve to further the right of everyone, regardless of frontiers, to express, seek, receive and impart information and ideas for the benefit of every individual and the democratic culture of any society (...)'.
³⁸ Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies, available at site www.coe.int.

³⁹ Declaration on Human Rights and the rule of law in the Information Society, adopted by the Committee of Ministers on 13 May 2005 at the 926th meeting of the Ministers' Deputies, available at site www.coe.int.

⁴⁰ Recommendation CM/Rec(2007)11 of the Committee of Ministers on promoting freedom of expression and information in the new information and communications environment, adopted by the Committee of Ministers on 26 September 2007 at the 1005th meeting of the Ministers' Deputies, available at site www.coe.int.

⁴¹ Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on measures to promote the respect for freedom of expression and information with regard to Internet filters, adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies, available at site www.coe.int.

forbids access to specific Internet content may constitute a restriction on freedom of expression and access to information in the online environment and that such a restriction would have to fulfil the conditions in Article 10, paragraph 2, of the European Convention on Human Rights and the relevant case-law of the European Court of Human Rights', urges the Member States to 'guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights'.

3. The scope of injunctions

It follows from the foregoing that the European Community and the Europe of Human Rights come together in a common desire to promote information society services and, more broadly, freedom of expression, shielded from all forms of prior censorship. To this dual end, the two Europes have sought to adjust the liability of intermediary providers downwards, by prescribing the following two bans:

- firstly, a ban on establishing liability of intermediaries in relation to information they transmit, host or store in cached form, providing certain conditions are met⁴²;
- secondly, a ban on imposing a general obligation on intermediaries to monitor the information they transmit or store, or a general obligation actively to seek facts or circumstances indicating illegal activity.⁴³ Framed in absolute terms, subject solely to the proviso contained in recital 47 (see below, paragraphs 31 and 32), this provision is similarly addressed to all national authorities: legislators, administrative authorities and courts; it concerns both courts ruling on the merits and those ruling on urgent applications.

This dual ban is not, however, an obstacle to the possibility, for judicial or administrative authorities, of ordering intermediaries to terminate or prevent an infringement committed using their services.

The Directive on electronic commerce, in fact, states that the rules on exemption of intermediary providers from liability, subject to conditions, 'shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement'.⁴⁴ The Declaration on freedom of communication on the Internet sets out a similar principle: 'In all cases, the above-mentioned

limitations of liability should not affect the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of the law'.⁴⁵

It should be noted that the decision to prescribe measures intended to oblige intermediaries to prevent or terminate an infringement is left to Member States: it is for national legal orders to determine whether, and in what circumstances, such measures may be undertaken. That said, Article 18(1) of the Directive on electronic commerce establishes that Member States must ensure 'that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved'.

Subsequently, two European directives confirmed the possibility of seeking interim measures against intermediaries specifically in the field of enforcement of intellectual property rights.

Directive 2001/29 states that 'Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right'.⁴⁶

Directive 2004/48, for its part, extends this possibility to all intellectual property rights,⁴⁷ stating that 'Member States shall also ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC'.^{48,49}

This same Directive specifies, in Article 2, that it 'shall not affect (...) Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular'.

⁴⁵ Last paragraph of Principle 6.

⁴⁶ Article 8(3) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJEC, L 167 of 22 June 2001, p. 10. Emphasis added. See also recital 59 of the Directive.

⁴⁷ In the internationally recognised sense of the expression, i.e. including what we call industrial property (notably trade mark rights).

⁴⁸ Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJEC, L 195 of 2 June 2004, p.16. Emphasis added. See also recitals 22 and 23 of the Directive.

⁴⁹ Transposition of Directive 2004/48 into Belgian law required adaptation of the Law of 30 June 1994 on copyright and related rights (MB, 27 July 1994, p. 19297), Article 87(1) of which now reads as follows: 'The president of the court of first instance and the president of the commercial court, in the matters under the respective jurisdiction of these courts, shall establish the existence and order the termination of any infringement of a copyright or related right. They may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right (...)'. The text of the Benelux Convention on Intellectual Property (Trade Marks and Designs) has also been adapted to this same Directive. Article 2.2(6) of the BCIP (new version) states that 'The court may, at the request of the holder of a trade mark, issue an injunction for cessation of services against intermediaries whose services are used by a third party to infringe its trade mark right'.

⁴² Articles 12 to 14 of Directive 2000/31 and the Declaration of 28 May 2003 on freedom of communication on the Internet, Principle 6. Cf. above, paragraph 16.

⁴³ Article 15(1) of Directive 2000/31 and *ibid*.

⁴⁴ Cf. Articles 12(3), 13(2) and 14(3), as well as recital 45, of the Directive on electronic commerce.

Hence the following question: how is the ban on national courts imposing a general monitoring obligation on intermediary providers to be reconciled with the possibility granted to them to issue an injunction against these same intermediaries in cases where a third party uses their transmission or storage services to infringe an intellectual property right?

There seems to be a need to explore the notion of a general monitoring obligation more deeply at a conceptual level (A) and in the light - or, rather, through the *chiaroscuro* - of case-law (B) in order to be able to define precisely the scope of injunctions (C).

3.1. Lack of a general monitoring obligation: what does it mean?

In order properly to understand the scope of the ban on imposing a general monitoring obligation on intermediaries, it is important to define the outline of that obligation (1) before distinguishing it from a specific monitoring obligation (2).

3.1.1. Outline of the general monitoring obligation

Benefit from exemptions from liability, introduced - subject to conditions - for intermediary providers, would have been reduced virtually to nil if they had not been supplemented by the principle of a ban on any general monitoring obligation. This is because, in the absence of such a principle, some States could have been tempted to impose on intermediaries, particularly host providers,⁵⁰ a general obligation actively to seek facts or circumstances indicating illegal activities. Case-law confirms that such a temptation is not illusory, far from it (see below, paragraph 2). Thus obliged to flush out infringements committed using their services, intermediaries would inevitably have practised prior censorship, including where content was legitimate, through fear of being made liable.⁵¹

It would not have made sense for the European legislator to tolerate an intermediary removing information on the basis of mere suspicion of its illegality or simple denunciation, without having first obtained confirmation of its illegal nature from an independent third party. Such an approach, difficult to reconcile with a respectful understanding of freedom of expression and the public's right to information,⁵² would have damaged the basic principles of

a democratic society.⁵³ These considerations reinforce the fact, already clear, that no condition may be added to those prescribed by Articles 12 – 14 of the Directive on electronic commerce.⁵⁴ They also confirm that the ban under Article 15 (1) concerns not just courts ruling on the merits but also those ruling on urgent applications.

Moreover, without an explicit ban on imposing a general monitoring obligation on intermediaries, there was a very real risk of sliding towards objectivisation of their (civil) liability, so great would the temptation have been for courts, in the presence of illegal information, to assume inadequate supervision and, from this, to deduce fault on the part of the intermediary under criticism. This attitude, in line with the trend in ideas on civil liability, would have been the opposite of what was intended by the European legislator. This shows that the two bans referred to above necessarily go hand in hand and are mutually reinforcing.

3.1.2. What form of monitoring is covered?

By banning the imposition of a general monitoring obligation on intermediary providers, the European legislator must have had blocking and filtering software in mind. It must have been clear to the legislator that a general monitoring obligation is only possible using technical equipment in the digital environment.⁵⁵

This fact is established beyond doubt by the European Commission's First Report on Directive 2000/31⁵⁶ and the

⁵³ P. Trudel, 'La responsabilité des acteurs du commerce électronique', in V. Gautrais, *Droit du commerce électronique*, Montreal, publ. Thémis, 2002, pp. 607–649, specifically paragraphs 66 to 68, commenting on the Canadian arrangements analogous to those established by Articles 12 to 14 of the Directive on electronic commerce.

⁵⁴ Cf. the grounds relied on by the Commission to reject various amendments proposed during preparatory work on Directive 2000/31 (Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market, 17 August 1999, COM(1999)427 final, p. 8), as well as the Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003 on the application of Directive 2000/31/EC on electronic commerce, COM(2003)702 final, p. 14.

⁵⁵ In this regard, F. Coppens, 'Filtrage P2P: possibilités techniques et obstacles juridiques', RDTI, Issue 30, March 2008, p. 99; E. Montero, 'Chronique de jurisprudence en droit des technologies de l'information (2002–2008) - Droit du commerce électronique', RDTI, Issue 35, June 2009, p. 25. E. Crabit, who, as a European Commission official, was a front-line participant in drafting Directive 2003/31, writes this: 'This ban covers all types of general measures, even those that do not appear to be such but would have the same effect. In particular, this ban would cover measures requiring the host provider to undertake filtering of information it hosts, as well as a general monitoring obligation in a specific field, for example protection of minors' (*op. cit.*, p. 815. Emphasis added.).

⁵⁶ First Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003 on the application of Directive 2000/31 on electronic commerce, COM(2003)702 final, p. 14.⁷³

⁵⁰ As these are able to escape all liability in cases where they are not aware of facts or circumstances indicating illegal information or an illegal activity, some Member States could have sought to make them subject to an obligation actively to seek such facts or circumstances, which would have reduced the benefit of Article 14. In this regard, E. Crabit, 'La directive sur le commerce électronique. Le projet "Méditerranée"', RDUE, Issue 4, 2000, p. 815.

⁵¹ Cf. the Declaration on freedom of communication on the Internet of 28 May 2003, pp. 11 and 12 (see above, paragraph 16 *in fine*).

⁵² Recitals 9 and 46 of Directive 2000/31 clearly establish that the Directive is not meant to harm the fundamental principles of freedom of expression. If it had been possible to make intermediary Internet providers subject to a general obligation to monitor the information they transmit or store or a general obligation to seek facts or circumstances indicating illegal activity, this could have '[had] the effect of curbing freedom of expression' (Declaration on freedom of communication on the Internet, commentary on the sixth principle).

preparatory work on the act to transpose the Directive into Belgian law.⁵⁷

The ban in question is justified not just by the reasons of principle mentioned (safeguarding freedom of expression and avoiding preventive censorship),⁵⁸ but also on clear grounds of a practical and economic nature: general monitoring would be technically impractical and economically unsustainable.

As noted by the European Commission, '[this] is important, as general monitoring of millions of sites and web pages would, in practical terms, be impossible and would result in disproportionate burdens on intermediaries and higher costs of access to basic services for users'. 'However', it adds, 'Article 15 does not prevent public authorities in the Member States from imposing a monitoring obligation in a specific (...), individual case'.⁵⁹

The courts' power of injunction against an intermediary provider with a view to terminating or preventing an infringement cannot lead to a general monitoring order. Thus, any general filtering measure seems to be prohibited by Article 15(1) of the Directive. At most, national authorities may impose a specific monitoring obligation.

In this regard, the ambiguity of the expression 'or prevent an infringement'⁶⁰ is to be deplored. It leads to the idea that the Directive sanctions injunctions that consist in imposing an obligation to supervise/monitor disseminated content on a preventive basis. Given the risk of contradicting Article 15(1) of the Directive, intermediaries' preventive role may only be conceived fairly narrowly.⁶¹ It is clear that imposing a measure obliging an intermediary, explicitly or implicitly, to filter all content it transmits or stores so as to block supposedly illegal content, even if this illegality had not been established

beforehand in accordance with Article 6 ECHR, would be irreconcilable with the prohibition under Article 15(1).

How is recital 40 of Directive 2000/31 to be understood, whereby: '(...) the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC'?

This recital means that the exemptions prescribed for certain intermediary activities do not prevent providers from carrying out *voluntary* checks, notably in a dual endeavour to cooperate with the holders of intellectual property rights and to preserve their brand image.⁶² In no case may a lack of such systems place the intermediary at fault and establish its liability. To assert the contrary would amount to considering, implicitly but definitely, that it has a general monitoring obligation, which is prohibited by Article 15 of Directive 2000/31. It should be emphasised that no obligation of a general nature may be imposed, even on the basis of a specific legal text.

It is also possible to question the scope of recital 48 of Directive 2000/31, worded as follows: 'This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities'.

Does this text authorise national legislators to prescribe supervisory obligations for host providers *a priori*? This recital cannot be interpreted in a way that would ruin the general organisation of the arrangements introduced by Articles 14 and 15 of the Directive. And so it must be considered, in particular, that it cannot serve to establish a general *monitoring* obligation, prohibited by Article 15(1).⁶³ The 'duties of care' referred to in recital 48 concern types of measures other than a general monitoring obligation, such as an obligation to put in place a structure for receiving complaints or systems for alerting and notification of inappropriate or undesirable content (as exists, moreover, on various second-generation websites), etc. In any case, this must involve independent obligations, associated with a specific sanction, unconnected to the question of the intermediary's liability with regard to content.⁶⁴

But what is the possibility of imposing selective filtering aimed at blocking specific content denounced as illegal?

In other words, is the monitoring obligation general as soon as it involves a search of all content in order to block a single, supposedly illegal, item, or is it only general if it concerns monitoring all content in order to flush out every potentially illegal item of content?⁶⁵

This is the essence of the problem of interpretation.

⁵⁷ Cf. draft Law on certain legal aspects of information society services, preamble, *Doc. parl.*, Ch. repr., sess. ord. 2002–2003, No 2100/1, p. 48. Also in this regard, P. Van Eecke, 'De nieuwe wetgeving inzake elektronische handel. Een eerste commentaar', *RW*, 2003–2004, pp. 338–339.

⁵⁸ A. Strowel, N. Ide and F. Verhoestraete, 'La directive du 8 juin 2000 sur le commerce électronique : un cadre juridique pour l'Internet', *JT*, No 6000, 2001, p. 142, Issue 34; G.M. Riccio, *La responsabilità civile degli Internet providers*, Giappichelli, Turin, 2002, p. 70 (the author makes the pertinent observation that the charges and costs created by a general monitoring obligation would have the effect of keeping the Internet just for those persons able to sustain them. As a result, what is at stake here is the possibility of giving concrete form to the right to free expression of thought and, more broadly, to its dissemination. In other words, such an obligation, while bringing about an oligopolistic concentration of businesses, would lead to a senseless situation: the right to freedom of expression would only exist *de facto* where the means of exercising it were guaranteed).

⁵⁹ First Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003 on the application of Directive 2000/31/EC on electronic commerce, COM(2003)702 final, p. 14.

⁶⁰ Articles 12(3), 13(2) and 14(3) of Directive 2000/31.

⁶¹ In this regard, E. Montero, 'La responsabilità des prestataires intermédiaires sur les réseaux' in *Le commerce électronique européen sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Brussels, Bruylant, 2001, p. 284, No 532; G. Riccio, *Profili di responsabilità civile dell'Internet Provider*, Salerno, 2000, p. 89.

⁶² E. Montero, *ibid.*, p. 279; C. Verdure, 'Les hébergeurs de sites web : victimes ou régulateurs de la société de l'information ?', *DCCR*, Issue 60, 2005, p. 41.

⁶³ In this regard and for other considerations, E. Montero, *ibid.*, pp. 289–292; A. Strowel, N. Ide and F. Verhoestraete, *op. cit.*, p. 142, Issue 37.

⁶⁴ E. Crabit, *op. cit.*, p. 815.

⁶⁵ Such an alternative is well-expressed by R. Hardouin, 'Observations sur les nouvelles obligations prétoriennes des hébergeurs', available at site www.juriscom.net.

3.1.3. General monitoring obligation versus specific monitoring obligation

It should be noted, first of all, that the possibility granted to the national authorities of imposing a specific monitoring obligation on intermediaries cannot be regarded as an exception to the principle of a ban on general monitoring obligations.⁶⁶ Such an analysis would amount to acknowledging that a general monitoring obligation may be imposed in some circumstances. That is not what is meant here. It is worth drawing attention to the essentially dialectical nature of law, in the sense that affirmation of a principle often goes hand in hand with the formulation of other principles, which, having their own field and justification, supplement the first one, tempering its effects without, however, contradicting them.⁶⁷

The possibility of imposing a specific monitoring obligation must be seen as affirmation of such a corrective principle, supplementing the principle of a ban on general monitoring measures without contradicting it. In other words, imposition of a general monitoring obligation does not seem to us to be allowed, even for the purposes of detecting specific content, within the possibility of imposing specific monitoring.

The fact remains that it is difficult, in practice, to make a distinction between a general monitoring obligation and a specific monitoring obligation. In this regard, the preparatory work and the actual text of the Directive are not very enlightening.

At most it may be considered, in light of recital 47 and some indications in the preparatory work for Directive 2000/31, that the ban on imposing general monitoring does not concern the monitoring obligations prescribed by a law applicable to a specific circumstance. This brings to mind, in Belgian law, Article 90b of the Code of Criminal Procedure: on this basis an investigating judge could order an intermediary to monitor a specific customer ('electronic listening'⁶⁸). In any case, only monitoring that is 'targeted' (clearly specified site, content) and 'temporary' is permissible, imposed at the request of national judicial or police authorities in order to prevent or tackle a specific illegal activity.⁶⁹

3.2. Illustrations through a critical review of case-law

In order to illustrate our proposition, it seems worth returning to a few cases of particular significance, brought before courts in France⁷⁰ (1), Germany (2) and Belgium (3).

⁶⁶ Comp. R. Ardouin, *ibid.*

⁶⁷ Cf. E. Bertrand, 'Le rôle de la dialectique en droit positif privé', D, 1951, chron. XXXV, pp. 151–154.

⁶⁸ This involves intercepting digital data during transmission.

⁶⁹ Article-by-article commentary on the Directive on electronic commerce, *op. cit.*, p. 31: 'This general rule does not exclude the possibility of a court or the police asking a service provider to supervise, for example, a specific site during a given period, in order to prevent or tackle a specific illegal activity'. See also the first draft of Article 15(1) in the Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, submitted by the Commission on 18 November 1998, COM (1998), 586 final.

⁷⁰ Some of these cases have been commented on by E. Montero, 'Les responsabilités liées au Web 2.0', *op. cit.*, p. 383 et seq.

3.2.1. French case-law

Among the abundant case-law an initial case appears of interest for our proposition. Copies of the film 'Joyeux Noël' had been discovered on Dailymotion, a video-sharing site. While acknowledging that the site manager was a host provider, the court seized of the case nevertheless considered the company liable on the ground 'that it must be seen as at least aware of facts and circumstances suggesting that illegal videos were being put online; that it therefore has to assume liability, being unable to put the fault back onto the users alone, since it deliberately provided them with the means to commit it'.⁷¹ Revealing a certain unease, the Court continues: 'whereas the law does not impose on technical providers a general obligation to seek facts and circumstances indicating illegal activities, this limitation does not apply when the said activities are generated or brought about by the provider itself; whereas it must be observed in the case in issue that the company Dailymotion did not implement any appropriate means to make access to the film 'Joyeux Noël' impossible (...), even though it was incumbent on it to undertake a priori supervision'.

This judgment calls for a number of criticisms. Two grounds for conviction are put forward in an incoherent way. The arrangements for host providers concern 'effective knowledge of illegal activity or information', i.e. of specific content. The Court is wrong to consider that the provider loses the benefit of the exemption from liability prescribed for hosting activity from the time it becomes aware of the mere possibility that illegal information may be put online on the exchange site. It would have been a different thing - acceptable in principle - to have considered the site owner at fault in the design of the platform. However, it cannot be found at fault within the meaning of Article 1382 of the Civil Code purely on the ground that it puts a platform at the disposal of Internet users, knowing that Internet users could download illegal content there. Such an analysis would amount, in practical terms, to condemning all content-sharing sites as a matter of principle ...⁷² Moreover, the supposed obligation of a priori supervision, indicated by the Court, is open to criticism on three counts: it makes the benefit of the prescribed exemption for hosting subject to a condition that does not figure in Article 14 of Directive 2000/31; it seems difficult to reconcile it with Article 15(1) of the same Directive; it is to be viewed with reserve in light of Article 10 ECHR.

By means of a carefully reasoned judgment of the Paris Court of Appeal of 6 May 2009, this decision has fortunately been altered in that the Court of Appeal found the company Dailymotion liable for putting the disputed content online since it had a priori knowledge of its illegal nature.⁷³

Another judgment delivered in France, in the 'Google video' case, merits criticism.⁷⁴ In the case in issue, a document produced by the company Zadig Productions had been disseminated via Google video, without its authorisation. When the producer notified Google of this dissemination,

⁷¹ T.G.I. Paris [Paris Court of First Instance] (3rd ch.), 13 July 2007, *Nord Ouest Production v S.A. Dailymotion*, cited above.

⁷² Comp. A. Saint Martin, *op. cit.*, p. 38.

⁷³ Paris (4th ch., A), 6 May 2009, *Nord Ouest Production v S.A. Dailymotion*, www.legalis.net.

⁷⁴ T.G.I. Paris (3rd ch.), 19 October 2007, *Zadig Productions et al. v Google Inc, Afa*, www.legalis.net.

Google was quick to remove the work. However, the film was put back online several times by various Internet users. Advised of each new instance of dissemination, Google systematically exercised due care in removing the film. Irritated when it was put online for the umpteenth time, Zadig decided to bring proceedings against Google video. The court considered that Google was acting as host provider and not as publisher. This status did not, however, prevent it from remaining liable, on the ground that ‘informed of the illegal nature of the content at issue by means of the first notification, it was for it to implement all necessary means to avoid further dissemination’. The means in question probably refer to implementation of a filtering measure. This decision seems very much open to criticism in that it makes the provider’s exemption from liability for the hosting activity subject to a condition not prescribed by the text of Article 14(1) of the Directive.⁷⁵ It must be acknowledged that it infringes not just this provision but also Article 15(1) of the Directive and, indeed, Article 10 ECHR. It was therefore wrong to have retained Google’s liability on the basis that it had not undertaken such supervision on its own initiative.

The following question also arises: in the context of an action for interim measures, could a court have imposed filtering aimed at avoiding further dissemination? Would such a measure have been reconcilable with Article 15(1) of the Directive?⁷⁶ Insofar as the host provider would not be required to filter all stored content but solely that notified, it could, just possibly, be maintained that this concerns a specific monitoring obligation. It would also be necessary for the monitoring imposed to be time-limited.⁷⁷ All in all, if the order involves filtering, on a temporary basis, of content that is specific, clearly identified and held (on a provisional basis) to be illegal, such a measure may seem legitimate in relation to Directive 2000/31. Be that as it may, it is also necessary to verify that it does not entail infringing Article 10 ECHR (see below, paragraph C).

On the same grounds we also have reservations concerning the judgment delivered in the case *Flach Film v Google*.⁷⁸ After having considered that, in operating the ‘Google video’ service, the well-known search engine was acting in the capacity of host provider, the court nevertheless considered that company to be liable on the basis of having committed acts of counterfeiting in allowing, via various links, the film ‘The World According to Bush’ to be downloaded or viewed via streaming. This conviction took place notwithstanding the promptness with which the links were removed as soon as their illegal nature was notified, since the court considered that Google was under ‘a monitoring obligation, specific to an extent, once it became aware of the illegal nature of the content’.

The court seems to have been more inspired in a case relating to the online advertising platform ‘Vivastreet’.⁷⁹ A number of perfume companies had noted the dissemination

via Vivastreet of advertisements offering sale of their perfumes outside the selective distribution network. By means of two interim orders, the Paris Commercial Court ordered removal of the disputed advertisements and the introduction, for a period of six months, of an *a priori* filtering system enabling detection and removal of advertisements relating to products of the brands concerned. However, here too, the measure restricting freedom of expression could come up against the triple test arising from Article 10 ECHR and, more specifically, the proportionality condition (see below, paragraph C).

3.2.2. German case-law

Counterfeit watches of the ‘Rolex’ brand had been put up for auction on the marketplace sites ‘Ricardo.de’ and ‘eBay.de’.

By means of three successive judgments, the *Bundesgerichtshof* considered that a host provider, aware of the illegal nature of stored information, had a duty not just to remove it but also to take reasonable filtering measures to prevent future storage of information of that type. Otherwise, the host provider was committing a fault making it liable in relation to illegal information that could not have been accessed if ‘efficient’ (?) filtering had been implemented.⁸⁰

These judgments are clearly open to criticism in that the benefit of exemption from liability introduced for the intermediary in relation to stored information is not granted solely under the heading and conditions of Article 14(1) of Directive 2000/31, but is made subject to compliance with a supplementary condition, not prescribed by that text.

3.2.3. Belgian case-law

Belgian case-law is distinguished by two disastrous judgments in a case pitting SABAM against the access provider Tiscali (now Scarlet). Using Article 87(1) of the Law on copyright,⁸¹ SABAM, the Belgian copyright management company, sought a judgment against Tiscali requiring it to terminate copyright infringements concerning musical works in its catalogue due to non-authorised exchange of musical files, carried out using peer-to-peer (P2P) software via the access provider’s services.

In an interlocutory judgment of 26 November 2004, the Brussels Court of First Instance considered that Article 87(1) indeed offered sufficient basis for a judgment ordering an intermediary to terminate a copyright infringement, providing this was specific, circumscribed and duly established. We, however, take the contrary view that such a measure, involving a general and permanent filtering obligation aimed at neutralising *peer-to-peer* networks, contradicts the letter and spirit of the Directive on electronic commerce. Thus we regretted the fact that the court implicitly acknowledged that it was legally possible to impose a general filtering obligation on Tiscali, aimed at preventing future copyright infringements, while we welcomed its decision to suspend its ruling until it

⁷⁵ Article 6.1.2 and 3 of Law No 2004-575 of 21 June 2004 on confidence in the digital economy.

⁷⁶ Article 6.1.7 of the Law on confidence in the digital economy.

⁷⁷ Comp. R. Hardouin, ‘Observations sur les nouvelles obligations prétoriennes des hébergeurs’, cited above.

⁷⁸ Comm. Paris, 20 February 2008, www.legalis.net.

⁷⁹ Comm. Paris (ref.), two judgments, 26 July 2007 and 31 October 2007, *Kenzo et al. v DMIS*, www.legalis.net.

⁸⁰ BGH, 11 March 2004, *Rolex v Ricardo* (Case ‘Internet-Versteigerung I’), I ZR 304/01, MMR, 2004, 668; BGH, 19 April 2007, *Rolex v eBay* (Case ‘Internet-Versteigerung II’), I ZR 35/04; BGH, 12 July 2007, *IDV v eBay*, I ZR 18/04.

⁸¹ Law of 30 June 1994 on copyright and related rights, MB, 27 July 1994, p. 19297.

received more information about the feasibility and effectiveness of the measures sought by SABAM.⁸²

By means of a further judgment of 29 June 2007, the same court ordered Scarlet to terminate the copyright infringements established in the judgment of 26 November 2004 by rendering impossible all forms of exchange by its customers, using P2P software, of files containing a musical work from SABAM's catalogue, on pain of a fine of EUR 2500 a day if Scarlet did not comply with the judgment after expiry of a time-limit of six months following its service.⁸³

Notwithstanding the reservations expressed by the expert witness, the court found that technical measures were in fact available to neutralise the copyright infringements established on the network to which Scarlet provided access. Specifically, these concerned digital fingerprinting technology developed by the company Audible Magic.⁸⁴ The court was wrong, in particular, to reject the argument whereby the technical measures sought would amount to imposing on Scarlet a general monitoring obligation, prohibited by Article 15(1) of the Directive on electronic commerce.⁸⁵ This provision did not rule out the use of filtering tools, in the court's view, in light of recital 40 of the Directive on electronic commerce. Moreover, Article 15 was addressed solely to the court ruling on liability and the injunction would not require Scarlet to 'monitor' its network. However, as already suggested (see above, paragraph 28), the passage regarding technical surveillance instruments cannot be arbitrarily isolated within recital 40, which, read as a whole, undoubtedly refers to 'voluntary agreements' between all parties concerned. Moreover, since Article 15 is expressed in absolute terms and without exception, it is addressed to all national authorities, including courts hearing interim applications (see above, paragraphs 20 and 25). Lastly, it is undeniable that network monitoring is imposed on Scarlet on the pretext that it operates using technical instruments: how could it have been otherwise in the digital universe?

The case did not end there since, in the meantime, the Brussels Court of First Instance, seized for the purpose of interim measures, decided to cancel the fines payable by Scarlet for the current period from January to 31 October 2008.⁸⁶ Moreover, Scarlet appealed against the judgments delivered on 26 November 2004 and 29 June 2007. The ninth chamber of the Brussels Court of Appeal, called upon to rule

on this appeal, decided to refer two questions to the Court of Justice of the European Union for a preliminary ruling.⁸⁷ The first was worded as follows: 'Do Directives 2001/29 and 2004/48, read in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 ECHR, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: 'They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right', to order an Internet Service Provider (ISP) to introduce, for all its customers, in *abstracto* and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?'

The answers from the CJEU will clearly be of very great interest for our proposition.

The judgment delivered on 31 July 2008 by the Brussels Commercial Court in the case *Lancôme v eBay* is much more satisfactory. Having noted the posting of illegal offers of sale on the site managed by eBay, *Lancôme* accused the well-known auction site of failing to take effective measures to combat counterfeiting of its perfumes and brought proceedings against it. Adopting a 'mixed classification', consisting in distinguishing the applicable liability arrangements according to the nature of the disputed activity, the court found that eBay benefited from the exemption from liability prescribed under the heading and conditions of Article 14 of the Directive⁸⁸ in relation to sales advertisements posted on its site by third parties, while having to assume liability under ordinary law with regard to the other services offered (which were not criticised by *Lancôme*).

The court also specified, rightly, that, in accordance with Article 15 of the Directive on electronic commerce (Article 21 of the Belgian Law), eBay does not have to assume 'any obligation to monitor the information it hosts, nor any general obligation actively to seek facts or circumstances indicating illegal activity.' As a result, *Lancôme's* application, aimed at banning eBay from allowing various types of advertisements to be posted on its site, which would require monitoring that cannot be imposed on it, was not allowed.⁸⁹

To see the principles correctly applied, reference may also be made to an exemplary judgment of the Antwerp Court of Appeal of 20 December 2006, an extract from which is worth

⁸² See E. Montero and Y. Cool, 'Le "peer-to-peer" en sursis ?', commentary on Civ. Brussels (cess.), 26 November 2004, RDTI, Issue 21, 2005, pp. 97–106.

⁸³ Civ. Brussels (cess.), 29 June 2007, AM, 2007/5, p. 476, RDC, 2007/7, p. 701, IRDI, 2007, p. 442, RDTI, Issue 30, 2008, p. 87, commentary by F. Coppens.

⁸⁴ This sophisticated technology forms part of the new generation of filtering tools: it aims to identify, among content hosted or transmitted on a network, protected works, via their digital representation and by comparison with the digital fingerprints of content covered by intellectual property rights supplied by the right holders and assembled in a vast data base; when content matching a digital fingerprint found in the data base is identified on the network or on a hosting site, that content is blocked.

⁸⁵ Article 21 of the Belgian Law of 11 March 2003 on certain legal aspects of information society services. For other reflections on the judgment, see in particular the commentary by F. Coppens cited in the footnote above.

⁸⁶ Civ. (ref.) Brussels, 22 October 2008, unpublished.

⁸⁷ Brussels (9th ch.), 28 January 2010, unpublished, RG 2007/AR/2424.

⁸⁸ Article 20 of the Belgian Law of 11 March 2003 on certain legal aspects of information society services.

⁸⁹ For other comments, see E. Montero, 'Sites de vente aux enchères et offres de vente illicites', commentary on Comm. Brussels (7th ch.), 31 July 2008, RDTI, Issue 33, 2008, pp. 528–533, and C. De Preter, 'Une salutation au jugement *Lancôme/eBay*, la visière levée', IRDI, 2008, pp. 253–255.

reproducing here: 'A ban on wider dissemination involves a monitoring obligation that is impractical and contrary to the letter of the Law on electronic commerce. A supplier of Internet services cannot be required actively to seek facts and circumstances indicating illegal activity. The measures ordered by the court may in no circumstance have the effect that publication, dissemination or issuing of an opinion, by whatever means of communication, is obstructed or made subject to conditions. The measure may therefore only consist of removing the columns [...] that are the subject of these proceedings. There may be no question of obstructing future publication of other columns that could harm reputation and honour, which would constitute prior censorship'⁹⁰.

3.3. What type of injunction may be issued against intermediaries?

What is the scope of Article 11 of the Directive on intellectual property rights, given that it does not seek to affect Directive 2000/31, which, as has been seen, enshrines the possibility for a court to require an intermediary to terminate or prevent an infringement (Articles 12(3), 13(2) and 14(3)), while at the same time banning the court from imposing on it a monitoring obligation of a general nature (Article 15(1))? It is now time to capitalise on the lessons drawn from the theory and case-law expounded (see above, points A and B) in order to assess the scope of injunctions liable to be issued against an intermediary whose services are used to infringe an intellectual property right (trade mark right, copyright or related right, etc.).

It only seems possible to envisage a form of injunction that involves specific acts of removal, blocking or filtering relating to an infringement, or risk of infringement, which is identified, clearly circumscribed and duly established. Such will be the case, for example, in situations where a site contains counterfeited works, particularly if it is hosted anonymously: where the owner of the disputed site cannot be identified, the intermediary may be instructed to remove the counterfeit content. A host provider could also be ordered to cease storing an illegal site or access providers to implement all appropriate measures to prevent access to the disputed site from national territory.⁹¹

On the other hand, where it involves permanent security or filtering measures, an injunction aimed at banning a type of infringement (such as hosting offers of counterfeit products of a particular brand, blocking illegal exchange of music files, etc.) would contradict not just the principle of prohibiting any general monitoring obligation but also the fundamental principles concerning freedom of expression, which includes freedom to receive and impart information - without censorship (Article 10 ECHR). In fact, as illustrated by a number of cases referred to above, given that all types of infringements would, sooner or later, be committed via the services of any sizeable carrier or host provider, injunctions aimed at banning each type of infringement are likely to multiply. And yet, the spirit and letter of the Directive on electronic commerce

clearly rule out the possibility of filtering imposed on an intermediary, intended to detect all supposedly infringing content, becoming an instrument in the general fight against infringement of intellectual property rights.⁹²

In fact, imposition of a filtering measure is highly likely to infringe the right to freedom of expression. For interference in this right to be permissible in light of the European Convention, it must be prescribed by law, pursue one of the legitimate objectives restrictively listed in Article 10(2) of the Convention and meet a proportionality requirement.

It is difficult to argue with the fact that European legislation provides for the possibility of an injunction. Even so, it could be argued that the possibility of filtering does not emerge clearly from a combined reading of the various texts and that case-law is not very clear on this question. Are intermediaries thus in a position to predict, with a sufficient degree of certainty, the consequences that might result from behaving in a particular way (see above, paragraph 11)? Even by surrounding themselves with enlightened advice, Internet intermediaries do not seem to be in a position to predict, to a reasonable degree, that a filtering measure, even limited to specific content, may be imposed on them.

What, then, of the two other conditions of legitimacy and proportionality?

The legitimate objective of protecting the rights of others appears in the second paragraph of Article 10. What is more, as has been seen, the Court recently acknowledged that intellectual property rights fall within the scope of Article 1 of the First Additional Protocol to the Convention, which protects the right to property.

The third condition, 'proportionality', therefore remains. Implementation of this condition cannot give rise to an assessment that is guided solely by intuition or common sense and, consequently, that is eminently subjective. In light of the pioneering role played by German administrative case-law, it may be considered that conformity with the proportionality criterion assumes, more specifically, that three conditions are met⁹³: the measure restricting freedom must be *appropriate*, i.e. such as to protect effectively the legitimate interest harmed by exercise of this freedom⁹⁴; it must also be *necessary*, in the sense that, among the various means suitable for achieving the pursued objective, the measure chosen is the one least damaging to the rights involved; lastly, it must satisfy the test of *proportionality stricto sensu*, i.e. there is still a need to demonstrate that the restricted freedom does not outweigh the legitimate interest to be safeguarded or, in other words, that

⁹² In this regard, S. Dusollier, 'Tribune libre - Responsabilités des intermédiaires de l'Internet: un équilibre compromis?', RDTI, Issue 29, 2007, pp. 269–272.

⁹³ Cf. S. Van Drooghenbroeck, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux*, Brussels, Bruylant, 2001, specifically pp. 31–38, and the numerous references; F. OST and M. Van De Kerchove, *De la pyramide au réseau. Pour une théorie dialectique du droit*, Brussels, Publications des F.U.S.L., 2002, p. 440 and the reference to H. Maurer, *Droit administratif allemand*, translated by M. Fromont, Paris, LGDJ, 1995, p. 272.

⁹⁴ The measure will be judged inappropriate if it is shown that, on the date it was taken, it was bound to fail in normal circumstances. Cf. S. Van Drooghenbroeck, *op. cit.*, p. 35, No 31.

⁹⁰ Antwerp, 20 December 2006, AM, 2008, p. 138.

⁹¹ For an illustration see Cass. fr. (1st civ. ch.), 19 June 2008, unpublished, dismissing the appeal entered against the judgment delivered on 24 November 2006 by the Paris Court of Appeal (14th ch., B) in the *aaargh* case, taken from the name of a negationist site.

the harm caused to the person entitled to the freedom who is concerned by the measure is not excessive in relation to the benefit it produces elsewhere. This balancing of conflicting freedoms or interests must take place not in the abstract, given that no interest protected by the Convention has absolute priority over the others, but according to the circumstances of each particular case.

Are the filtering measures imposed on intermediaries proportionate to the objective of protecting intellectual property rights?

As things stand, two observations are called for.

Firstly, filtering measures, even limited to specific content, do not seem suitable for effectively guaranteeing the anticipated result.⁹⁵ Ill-intentioned Internet users have more than one string to their bow and redouble their imaginative efforts to design circumvention strategies. It is thus common for a site's closure for infringing intellectual property rights of a third party to lead to the illegal activities transferring to another address. One way or another, is there not a risk of seeing the same illegal content endlessly returning to the Web? Filtering measures, far from being a panacea, would then only offer a brief respite...

Secondly, given the current state of the technology, most filters do not seem suitable for determining whether a communication is authorised or infringes intellectual property rights.⁹⁶

As a result, filtering measures, even limited to specific content, will practically always be 'over-inclusive' or 'under-inclusive'⁹⁷: they inevitably risk either leading to removal or blocking of content that in no way infringes intellectual property rights (this brings to mind communications justified by an exception to copyright, such as parody, or by a licence), or letting illegal communications through.

Imposition of filtering, even if limited, is very likely to be a measure disproportionate to the objective of protecting the rights of holders of intellectual property rights.

The current trend towards voluntary filtering,⁹⁸ notably on the basis of negotiated compromises between Internet intermediaries and right holders or their representatives, also calls for some reservations with regard to preserving the right to freedom of expression.

Of course, this in no way involves a State body imposing a filtering measure. It is however always under their positive

obligations (see above, paragraph 10), and pursuant to the theory of 'dissuasive effect',⁹⁹ that States should, to comply fully with Article 10 of the European Convention on Human Rights, ensure that they do not place intermediaries under such fear of liability claims that they come to impose on themselves filtering that is appropriate for making them immune to any subsequent accusation but is of a kind that threatens the freedom of expression of Internet users.

4. Conclusion

It is remarkable to note the extent to which the European Union and the Council of Europe are in agreement in considering that safeguarding and promoting freedom of expression, including the freedom to receive and impart information itself, demand both:

- a limit on the liability of information society intermediaries in the wording and the conditions of Articles 12 to 14 of the Directive on electronic commerce;
- a ban on imposing a general monitoring obligation on these same intermediaries.

In other words, the exemptions from liability and the banning rule referred to above arise from correct application of Article 10 ECHR, read in parallel with the various texts adopted within the framework of the Council of Europe. It is therefore in light of these principles and of the said Article 10 that the well-founded nature and the scope of injunctions liable to be issued against intermediary providers should be assessed. Indeed, the case-law developed by the Strasbourg Court around Article 10 shows that:

- this provision covers all types of information, including information of a commercial nature, and concerns not just the content of the information but also the means of transmission and reception (insofar as any restriction on these erodes the right to receive and impart information);
- exercise of freedom of expression, in its various forms, may only be made subject to certain conditions, restrictions or sanctions, necessary in a democratic society, if these are (1) prescribed by law, (2) justified by a pressing social need, and (3) proportionate to the goal legitimately pursued.

As has been seen, it is around the third condition, proportionality, that a delicate trade-off takes place between the right to freedom of expression and intellectual property rights.

In theory, the various texts of the European legal order show that a competent national authority of a Member State that has transposed Directive 2004/48 could, on establishing

⁹⁵ Cf., among other studies, C. Callanan, M. Gercke, E. De Marco, H. Dries-Ziekenheiner, "Internet blocking balancing cybercrime responses in democratic societies", 2009, www.aconite.com/blocking/study; M. Jayasuriya, J. Pearlman, R. Topolski, M. Weinberg, S. Siy, 'Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs', 2009, www.PublicKnowledge.org.

⁹⁶ It is true that recital 59 of Directive 2001/29, cited above, requires States to provide for the possibility of applying for an injunction 'even where the acts carried out by the intermediary are exempted under Article 5'. Nevertheless, it may be thought that this simply concerns the obligation to organise a right of appeal in favour of the holder of a copyright, enabling that person to allege infringement of his or her rights before a court without prejudice to the opposing party asserting an exception to copyright.

⁹⁷ M. Jayasuriya, J. Pearlman, R. Topolski, M. Weinberg, S. Siy, *op. cit.*, specifically p. 47 and p. 49.

⁹⁸ See C. Angelopoulos, *op. cit.*, pp. 9–10.

⁹⁹ See, in general terms, K. Lemmens, 'Se taire par peur : l'effet dissuasif de la responsabilité civile sur la liberté d'expression', *A&M*, 2005, pp. 32–40.

transmission or storage by an intermediary provider of information infringing an intellectual property right, issue an injunction against that intermediary, provided that the measures ordered only involve acts of monitoring, removal, disabling of access or filtering that relate to specific and clearly identifiable content, held to be illegal under an interim or final judgment made by a competent national authority and open to appeal before an impartial court or regulating body in accordance with Article 6 ECHR.

As things stand, despite technological progress and the emergence of software that is increasingly precise and ever better controlled in terms of its effects, implementation of a filtering measure appears difficult to reconcile with the right

to freedom of expression. How do we do enough without doing too much?

The question arises: does there really exist, at present, a technological possibility of filtering, directed towards specific and clearly identifiable content, that is both effective, i.e. such as to prevent recurring infringement of an intellectual property right, and appropriate for enabling the right to freedom of expression on the Net?

Etienne Montero (etienne.montero@fundp.ac.be) Professor at the University of Namur (Belgium) and Dean of the Faculty of Law & **Quentin Van Enis** (quentin.vanenis@fundp.ac.be) Teaching Assistant at the University of Namur (Belgium).